UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VANESSA VIGIL and RICARDO VIGIL, on behalf of themselves and all others similarly situated, Plaintiffs, v. TAKE-TWO INTERACTIVE SOFTWARE, INC., Defendant.	Civil Action No. 15-cv-08211-JGK **SECOND AMENDED CLASS ACTION COMPLAINT**

Plaintiffs Vanessa Vigil and Ricardo Vigil, individually and on behalf of all others similarly situated, bring this Class Action Complaint for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/1 to 14/99 (West, Westlaw through P.A. 99-324 of 2015 Reg. Sess.), against Take-Two Interactive Software, Inc. ("Take-Two"), and allege as follows based on personal knowledge as to themselves, on the investigation of their counsel and the advice and consultation of certain third-party agents as to technical matters, and on information and belief as to all other matters, and demand trial by jury:

NATURE OF ACTION

1. Take-Two is a publisher, developer and distributor of numerous video games, including the "NBA 2K15" and "NBA 2K16" video games for personal computers, the Sony PlayStation 4 and Microsoft Xbox One gaming platforms. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Take-Two in collecting, storing, using, disclosing and disseminating Plaintiffs' and other similarly situated individuals'

biometric identifiers[1] and biometric information[2] (referred to collectively at times as "biometrics") without informed written consent, in violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 Ill. Comp. Stat. 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics – particularly in the City of Chicago, which was selected by major national corporations as a "pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias," 740 Ill. Comp. Stat. 14/5(b) – the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Take-Two may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used, *see id.*; (3) receives a written release from the person for the collection of his or her biometric identifiers or information, *see id.*; and (4) publishes publically available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information, *see* 740 Ill. Comp. Stat. 14/15(a).

---

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans and "face geometry", among others. 740 Ill. Comp. Stat. 14/10.

[2] "Biometric information" is any information captured, converted, stored or shared based on a person's biometric identifier used to identify an individual. 740 Ill. Comp. Stat. 14/10.

4. In violation of each of the foregoing provisions of sections 15(a) and 15(b) of BIPA, Take-Two is actively collecting, storing and using – without providing adequate notice, receiving informed written consent or publishing data retention policies – the biometrics of thousands of Illinois residents.

5. Specifically, Take-Two has created, collected and stored "scans of face geometry" (or "face templates") – highly detailed geometric maps of the face – from thousands of Illinois residents. Both the NBA 2K15 and NBA 2K16 video games are equipped with software that, in combination with a camera attached to a personal computer or a game console, operates to extract and analyze data from the points and contours of the face of an individual playing the game, and thereafter creates a virtual player with a personally identifying facial rendition. Each face template, on which each rendition is based, is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person.

6. Plaintiffs bring this action individually and on behalf of all others similarly situated to prevent Take-Two from further violating the privacy, personal security and informational rights of Illinois residents, and to recover statutory damages for Take-Two's unauthorized collection, storage, use, disclosure and dissemination of biometrics in violation of BIPA.

PARTIES

7. Plaintiff Vanessa Vigil is, and has been at all relevant times, a resident and citizen of Chicago, lllinois.

8. Plaintiff Ricardo Vigil is, and has been at all relevant times, a resident and citizen of Chicago, lllinois.

9. Take-Two is a Delaware corporation with its headquarters and principal place of business in New York, New York. Take-Two is a citizen of the states of Delaware and New York.

JURISDICTION AND VENUE

10. Subject matter jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because: (i) the proposed class consists of well over 100 members; (ii) the parties are minimally diverse, as members of the proposed class, including Plaintiffs, are citizens of a state different from Take-Two's home states; and (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. There are likely tens of thousands of individuals who, while residing in Illinois, had their scans of face geometry and personally identifying information based on their scans of face geometry collected by Take-Two. The estimated number of individuals residing in Illinois who were impacted by Take-Two's conduct multiplied by BIPA's statutory liquidated damages figure ($5,000 for each intentional or reckless violation and $1,000 for each negligent violation) easily exceeds CAFA's $5,000,000 threshold.

11. This Court has personal jurisdiction over Take-Two because Take-Two maintains its corporate headquarters and principal place of business in New York, New York.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Take-Two maintains its corporate headquarters and principal place of business in this District.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

13. "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning an image of a human face (or scanning an actual person's face), extracting facial-feature data based on specific "biometric identifiers" (i.e., details about the face's geometry as determined by facial points and contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a "face template database." If a database match is found, an individual may be identified.

14. Facial recognition technology is capable of using biometric identifiers and information in ways that present numerous privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, Senator Al Franken expressed concern that facial recognition technology could be "abused in ways that could threaten basic aspects of our privacy and civil liberties."[3] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[4]

15. The Federal Trade Commission ("FTC") has raised similar concerns, and recently released a "Best Practices" guide for companies using facial recognition technology.[5] In the guide, the Commission underscores the importance of companies' obtaining affirmative, informed consent from consumers before extracting and collecting their biometric identifiers and biometric information.

16. The risk of harm resulting from a biometrics data breach cannot be understated. If a hacker were to compromise a company's database of biometric scans of face geometry, the hacker would have access to unchangeable customer data used to prove identity -- not only for that company, but for every company that has adopted that form of biometric authentication. With widespread adoption of biometric authentication in recent months, a single large hack could permanently compromise tens of millions of customers who would thereafter have no way to protect the integrity of their identities.

---

[3] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* http://www.franken.senate.gov/?p=press_release&id=2144.

[4] *Id.*

[5] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

17. As an article published in the July 13, 2016 edition of the New York Times explains, banks and all other companies that do business online are at risk of a data breach. That risk is especially great, and the resulting injury especially severe, if biometrics are involved:

> Hacking of banks and identities is big business. An estimated 17.6 million Americans were subject to identity theft in 2014, mostly through breached bank accounts and credit cards. At this point, bank hackers are probably not looking for biometric data when attacking a bank. But even if it leaks as a by-product of a financial breach, criminals will find ways to abuse biometric data or resell it for further exploitation. And biometric data is more sensitive than other personal information banks store on behalf of their customers because unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a person's face or fingerprints….
>
> If the compromised data happens to be biometrics, issues of identity theft may simply be unresolvable. … It is not enough for banks to simply avoid storing images of fingerprints, faces or irises. The biometric data that they get from processing those geometries (what banks call "templates") can also be abused if they are accessed in combination with the algorithm used to extract the templates from the original images.

Yana Welinder, *Biometrics in Banking Is Not Secure*, The New York Times, July 13, 2016 (available at http://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure).

18. As explained below (*see infra* Part III), Take-Two failed to obtain adequate consent from Plaintiffs or the putative Class members before collecting, storing, using, disclosing or disseminating their biometric identifiers and information through the NBA 2K15 and NBA 2K16 video games. Not only do Take-Two's actions fly in the face of FTC guidelines, they also violate the privacy, personal security and informational rights of Illinois residents, causing financial harm and a risk of severe harm in the process.

II. Illinois's Biometric Information Privacy Act

19. In 2008, Illinois enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Ill. House Tr., 2008 Reg. Sess. No. 276.

20. Specifically, The Illinois legislature's motivation for regulating scans of face geometry and other biometrics was based on its understanding that biometrics embody a person's immutable biological characteristics, and thus, unlike other identifiers, cannot be changed in the event of a security breach:

> Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.
>
> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.
>
> An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information[, . . . and are thus] deterred from partaking in biometric identifier-facilitated transactions.

21. BIPA makes it unlawful for a company to, inter alia, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[6] or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

[6] BIPA's definition of "biometric identifier" expressly includes "scans of face geometry." *See* 740 Ill. Comp. Stat. 14/10.

> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 Ill. Comp. Stat. 14/15(b).

22. Section 15(a) of BIPA provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 Ill. Comp. Stat. 14/15(a).

23. BIPA further provides that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 Ill. Comp. Stat. 14/15(c).

24. Moreover, BIPA provides that '[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric" without written consent. 740 Ill. Comp. Stat. 14/15(d).

25. Finally, BIPA requires private entities to "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry," and to protect them from disclosure in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." *Id.* 14/15(e).

26. As alleged below (*see infra* Part III), Take-Two's practices of collecting, storing, using, disclosing and disseminating biometric identifiers and information without first providing the requisite written disclosures or obtaining the requisite written releases, as required by section 15(b)

of BIPA, violates individuals' protected rights to privacy and personal security in their biometrics, and their protected right to information regarding the collection and storage of their biometrics. Take-Two's disclosure and dissemination of individuals' misappropriated biometric identifiers and information for a profit violates sections 15(c) and 15(d) of BIPA, causing individuals monetary harm. Take-Two's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of biometric identifiers and information also violates section 15(a) of BIPA. Take-Two's failure to safeguard individuals' biometrics in a reasonable manner, in violation of section 15(e) of BIPA, has exposed individuals to a grave risk of severe harm.

III. Take-Two Violates the Biometric Information Privacy Act

27. To provide a realistic animation in which a game player himself or herself appears to compete in an NBA basketball game with NBA players, the "MyPlayer" feature of NBA 2K15 and NBA 2K16 allows gamers to create a personalized basketball player that has a 3-D rendition of the gamer's face.

28. When MyPlayer is first used, the gamer is presented with a screen that states:

> Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay. By proceeding you agree and consent to such uses and other uses pursuant to the End User License Agreement.
> www.take2games.com/eula

If the gamer presses "Continue," the gamer is permitted access to the face scanning feature of MyPlayer. As discussed below, this screen fails to disclose Take-Two's most invasive use of the face scans and renditions created in MyPlayer, which is their indefinite storage on Take-Two servers.

29. Using the cameras connected to the gaming platforms on which NBA 2K15 and NBA 2K16 operate, the 3-D mapping process captures a scan of the gamer's face geometry, which is then used to disseminate a realistic, personally identifying facial rendition of the gamer's face

during multiplayer game play. Gamers need to get very close (6-12 inches) to the camera and slowly turn their heads 30 degrees to the left and to the right during the scanning process. The process of scanning the face takes about 15 minutes.

30. The scanning process results in Take-Two's proprietary technology extracting geometric data relating to the unique points and contours of each face. These scans of face geometry that Take-Two collects from gamers constitute biometric identifiers under section 14/10 of BIPA. *See* 740 Ill. Comp. Stat. 14/10 (defining "biometric identifier" to mean, inter alia, a "scan of . . . face geometry").

31. Take-Two then uses the scans of face geometry to store and disseminate realistic, personally identifying, animated renditions of the faces during multiplayer game play. These renditions constitute "information . . . based on an individual's biometric identifier," 740 Ill. Comp. Stat. 14/10, and are therefore "biometric information" under BIPA, *id.*

32. Take-Two fails to "inform[] the subject . . . in writing that a biometric identifier or biometric information is being collected or stored." 740 Ill. Comp. Stat. 14/15(b)(1). Take-Two does not inform gamers in writing that their face scans (biometric identifiers) are being collected or stored. Take-Two thus violates section 15(b)(1) of BIPA.

33. Take-Two fails to "inform[] the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used." *Id.* 14/15(b)(2). Take-Two does not inform gamers in writing of the specific purpose and length of term for which their face scans (biometric identifiers) are being collected, stored and used. Take-Two thus violates section 15(b)(2) of BIPA.

34. Take-Two fails to "receive[] a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." *Id.* 14/15(b)(3). Take-Two does not receive a written release executed by gamers who are the subjects

of the face scans (biometric identifiers) and animated renditions (biometric information). Take-Two thus violates section 15(b)(3) of BIPA.

35. Take-Two "disclose[s], redisclose[s], or otherwise disseminate[s] . . . biometric identifier[s] or biometric information" without obtaining the consent of "the subject of the biometric identifier or biometric information or the subject's legally authorized representative[.]" *Id.* 14/15(d). Take-Two transmits unencrypted scans of face geometry (biometric identifiers) via the open, commercial Internet, and not a secure network such as a virtual private network. Take-Two discloses and disseminates facial renditions (biometric information), which are based on scans of face geometry (biometric identifiers), during multiplayer game play. Take-Two thus violates section 15(d) of BIPA.

36. The unique personally-identifying facial renditions (i.e., biometric information) and face templates (i.e., biometric identifiers) that Take-Two collects from gamers, and then disseminates in conjunction with multiplayer game play, are valuable assets to Take-Two because they enhance the realism of Take-Two's multiplayer game play for the NBA 2K15 and NBA2K16 video games. Because the realism of the multiplayer game play for the NBA 2K15 and NBA2K16 video games is a material factor motivating a significant numbers of individuals' decisions to purchase the NBA 2K15 and NBA 2K16 video games, Take-Two "profit[s] from a person's or a customer's biometric identifier or biometric information." 740 Ill. Comp. Stat. 14/15(c).

37. Take-Two fails to "store, transmit, [or] protect from disclosure [its collected] biometric identifiers and biometric information using the reasonable standard of care within the [Take-Two's] industry," and fails to protect them from disclosure in a manner that is "the same as or more protective than the manner in which [Take-Two] stores, transmits, and protects other confidential and sensitive information." *Id.* 14/15(e). Take-Two thus violates section 15(e) of BIPA.

38. Take-Two has failed to develop a written, publicly available policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." *Id.* 14/15(a). To the contrary, Take-Two indefinitely stores each gamer's face scan (biometric identifier) on Take-Two's remote server for use and dissemination, in the form of a facial rendition (biometric information), during multiplayer game play. Take-Two has no retention schedule or guidelines for statutorily compliant, permanent destruction of such biometric information and biometric identifiers, much less a written, publicly available policy establishing such a schedule or guidelines. Take-Two thus violates section 15(a) of BIPA.

IV. The Experiences of Plaintiffs Vanessa Vigil and Ricardo Vigil

39. Plaintiff Ricardo Vigil purchased and played the NBA 2K15 video game in Illinois on a PlayStation 4 that he purchased, installed and otherwise set up in Illinois.

40. Plaintiff Vanessa Vigil played the NBA 2K15 video game in Illinois on the PlayStation 4 console that her brother, Plaintiff Ricardo Vigil, purchased, installed and otherwise set up in Illinois.

41. Both Plaintiffs used the "MyPlayer" feature during the course of their game play on NBA 2K15. Before using "MyPlayer", each Plaintiff pressed "Continue" when presented with the screen stating that "[y]our face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay."

42. Unaware of the true nature of Take-Two's face scanning technology, including its indefinite storage of scans of face geometry on a remote server, Plaintiffs each used the PlayStation Camera to create a scan of face geometry for use during multiplayer game play. Each Plaintiff was instructed by the game to look directly into the PlayStation Camera, at which point the PlayStation

Camera and the game scanned and analyzed each Plaintiff's face and extracted each of their biometric identifiers in the form of "scans of face geometry" (or "face templates"), comprised of geometric data relating to, inter alia, the unique contours of each Plaintiff's face and the distances between each Plaintiff's eyes, nose and ears.

43. Take-Two then transmitted and stored the resulting face templates on its remote server. Take-Two transmitted Plaintiffs' unencrypted scans of face geometry via the open, commercial Internet, and not a secure network such as a virtual private network. Take-Two stored Plaintiffs' face templates in a manner that associates their identity with their biometric data.

44. Using Plaintiffs' face templates (biometric identifiers), Take-Two then created and stored on its remote server personally identifying facial renditions of Plaintiffs (i.e., biometric information), for purposes of dissemination during multiplayer game play.

45. Each Plaintiff subsequently entered a multiplayer game, at which point each Plaintiff's facial rendition (i.e., biometric information) was disclosed and disseminated to other players.

46. Take-Two failed to inform either Plaintiff in writing of these collection and storage practices prior to collecting and storing their biometric identifiers and information.

47. Neither Plaintiff was informed by Take-Two in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used.

48. Neither Plaintiff, nor any legally authorized representative of either Plaintiff, executed or delivered to Take-Two a written release with respect to the collection, storage, use, dissemination or disclosure of biometric identifiers or biometric information.

49. Take-Two has no written, publicly available policy establishing a retention schedule and guidelines for permanently destroying, in a statutorily compliant manner, Plaintiffs' biometric identifiers and biometric information.

50. Take-Two failed to "store, transmit, [or] protect from disclosure" Plaintiffs' biometric identifiers and biometric information using "the reasonable standard of care within the [Take-Two's] industry," and failed to protect Plaintiffs' biometric identifiers and biometric information from disclosure in a manner that is "the same as or more protective than the manner in which [Take-Two] stores, transmits, and protects other confidential and sensitive information." *Id.* 14/15(e).

51. By collecting, indefinitely storing and disseminating Plaintiffs' biometric identifiers and biometric information without first obtaining the requisite informed consent, Take-Two violated Plaintiffs' substantive rights, afforded by BIPA, to privacy and personal security in their biometrics.

52. By failing to provide Plaintiffs with written disclosures informing them of the collection and storage of their biometrics (and the specific purpose and duration of such collection and storage) prior to collecting Plaintiffs' biometric identifiers or biometric information, Take-Two violated Plaintiffs' protected right to receive information about the purpose and duration of the collection and storage of their biometrics, as provided by BIPA.

53. The "MyPlayer" feature of the NBA 2K15 video game, which Take-Two advertised as a feature that gamers could use to create a personalized basketball player, was a material factor motivating Plaintiff Ricardo Vigil's decision to purchase the NBA 2K15 video game.

54. At the time Plaintiff Ricardo Vigil purchased the NBA 2K15 video game, Plaintiff Ricardo Vigil was unaware that Take-Two collected, stored and disseminated gamers' biometric identifiers and biometric information in connection with the "MyPlayer" feature of the video game.

55. Had Plaintiff Ricardo Vigil known, prior to making his purchase of the NBA 2K15 video game, that Take-Two would collect, indefinitely store, and/or disseminate his unique biometric identifiers and/or biometric information without his informed written consent in connection with his use of the "MyPlayer" feature of the NBA 2K15 video game, Plaintiff Ricardo Vigil would not have purchased the NBA 2k15 video game, for any price. After purchasing and opening the packaging on the NBA 2K15 video game, Plaintiff Ricardo Vigil had no option to return the video game for a monetary refund. Accordingly, Take-Two's violations of BIPA caused Plaintiff Ricardo Vigil to suffer tangible, monetary harm.

56. The unique personally-identifying facial renditions (i.e., biometric information) and face templates (i.e., biometric identifiers) that Take-Two collects from gamers, and then disseminates in conjunction with multiplayer game play, are valuable assets to Take-Two because they enhance the realism of Take-Two's multiplayer game play mode for the NBA 2k15 and NBA2k16 video games.

57. Indeed, Take-Two touts the realism of its multiplayer game play mode for the NBA 2k15 and NBA2k16 video games in the course of marketing, promoting and selling the games. The realism of the multiplayer game play mode for the NBA 2k15 and NBA2k16 video games is a material factor motivating a significant numbers of individuals' decisions to purchase the NBA 2k15 and NBA 2k16 video games.

58. By collecting Plaintiffs' biometric identifiers and biometric information without informing Plaintiffs and without obtaining Plaintiffs' express consent, in violation of BIPA, Take-Two misappropriated Plaintiffs' valuable personal property.

59. Plaintiffs' have suffered tangible, monetary harm stemming from Take-Two's misappropriation of their biometrics to market and sell the NBA 2k15 and NBA 2k16 video games for a profit, in direct violation of BIPA. *See* 740 Ill. Comp. Stat. 14/15(c) ("No private entity in

possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.").

60. At the time Plaintiffs used the "MyPlayer" feature of the NBA 2k15 video game, neither Plaintiff was unaware that Take-Two collected, stored and disseminated gamers' biometric identifiers and biometric information in connection with the "MyPlayer" feature of the video game.

61. In light of Take-Two's unauthorized misappropriation of Plaintiffs' biometric identifiers and biometric information -- sensitive data which Take-Two has indefinitely stored and tied to Plaintiffs' identities on its unsecure server, without using a reasonable standard of care for storing or transmitting such data -- Plaintiffs have become weary of participating in biometrics-facilitated transactions, and have in fact refrained from participating in biometric-facilitated transactions facilitated by, among other things, scans of face geometry.

62. Because Take-Two has transmitted, indefinitely stored and disseminated Plaintiffs' unencrypted biometrics and corresponding identifying information via the open, commercial Internet, and not a secure network such as a virtual private network, Plaintiffs have suffered and will continue to suffer a serious risk of severe, irreversible harm based on the high likelihood that Take-Two's biometrics database will ultimately be breached and cause Plaintiffs to suffer serious financial harm, breaches of security and identity theft. Take-Two, unfortunately, cannot guarantee the security of its biometric data any more than Target, Sony, or the Office of Personnel Management were able to ensure the security of their electronically-stored data.

CLASS ALLEGATIONS

63. **Class Definition**: Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All individuals users who, while residing in the State of Illinois, and while playing, using or otherwise interacting with the "NBA 2K15"

> and/or "NBA 2K16" video game(s), had their biometric identifiers, including "scans of face geometry" (or "face templates"), and/or biometric information, including personally identifying renditions of faces based on "face templates," collected, captured, received, or otherwise obtained and/or stored, and/or disclosed or disseminated, by Take-Two without (1) being informed by Take-Two in writing that a biometric identifier or biometric information was being collected or stored, (2) being informed by Take-Two in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used, (3) delivering to Take-Two an executed release pertaining to biometric identifiers and biometric information, and/or (4) Take-Two's establishment of a written, publicly available policy establishing a retention schedule and guidelines for permanently destroying, in a statutorily compliant manner, biometric identifiers and biometric information.

The following are excluded from the Class: (1) any Judge presiding over this action and members of their family; (2) Take-Two, Take-Two's subsidiaries, parents, successors, predecessors, and any entity in which Take-Two or its parent has a controlling interest (as well as current or former employees, officers and directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Take-Two's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

64. **Numerosity**: The number of persons within the Class is substantial, believed to amount to thousands of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

65. **Commonality and Predominance**: There are well defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do

not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member include, but are not limited to, the following:

(a) whether Take-Two collected or otherwise obtained Plaintiffs' and the Class's biometric identifiers or biometric information;

(b) whether Take-Two properly informed Plaintiffs and the Class that Take-Two collected or stored their biometric identifiers or biometric information;

(c) whether Take-Two properly informed Plaintiffs and the Class of the specific purpose and length of term for which Take-Two collected, stored, and used their biometric identifiers or biometric information;

(d) whether Take-Two obtained a written release (as defined in 740 Ill. Comp. Stat. 14/10) to collect, use, store, disclose or disseminate Plaintiffs' and the Class's biometrics identifiers or biometric information;

(e) whether Take-Two developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometrics information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever occurs first;

(f) whether Take-Two used Plaintiffs' and the Class's biometric identifiers or biometric information to identify them; and

(g) whether Take-Two's violations of BIPA were committed intentionally, recklessly, or negligently.

66. **Adequate Representation**: Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Neither of the Plaintiffs nor their counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs are able to fairly and adequately represent and protect the interests of such a Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

67. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class wide relief is essential to compel compliance with BIPA.

FIRST CAUSE OF ACTION
Violation of 740 Ill. Comp. Stat. 14/1 to 14/99
(On Behalf of Plaintiffs and the Class)

68. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

69. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information." 740 Ill. Comp. Stat. 14/15(b). BIPA also makes it unlawful for any private entity to, among other things, "disclose, redisclose, or

otherwise disseminate a person's or a customer's biometric identifier or biometric information." 740 Ill. Comp. Stat. 14/15(d).

70. Take-Two is a Delaware corporation and thus qualifies as a "private entity" under BIPA. *See* 740 Ill. Comp. Stat. 14/10.

71. Plaintiffs and the Class members are individuals who had their "biometric identifiers" (specifically, scans of face geometry) collected, stored and used by Take-Two. *See* 740 Ill. Comp. Stat. 14/10.

72. Plaintiffs and the Class members are individuals who had their "biometric information" (specifically, personally identifying facial renditions based on scans of face geometry) collected, stored and used by Take-Two.

73. Take-Two failed to properly inform Plaintiffs or the Class in writing that their biometric identifiers and/or biometric information was being collected and stored, nor did they inform Plaintiffs or the Class members in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information was being collected, stored, and used, as required by 740 Ill. Comp. Stat. 14/15(b)(1)-(2).

74. Take-Two systematically and automatically collected, stored and used Plaintiffs' and the Class members' biometric identifiers and/or biometric information without first obtaining the written release required by 740 Ill. Comp. Stat. 14/15(b)(3).

75. In addition, Take-Two does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiffs or the Class members, as required by BIPA. *See* 740 Ill. Comp. Stat. 14/15(a).

76. Take-Two systematically and automatically disclosed and disseminated Plaintiffs' and the Class members' biometric information without first obtaining adequate consent required by 740 Ill. Comp. Stat. 14/15(d)(1)-(3).

77. Take-Two failed to "store, transmit, [or] protect from disclosure" Plaintiffs' and the Class members' biometric identifiers and biometric information using "the reasonable standard of care within the [Take-Two's] industry," and failed to protect Plaintiffs' and the Class members' biometric identifiers and biometric information from disclosure in a manner that is "the same as or more protective than the manner in which [Take-Two] stores, transmits, and protects other confidential and sensitive information," as required by 740 Ill. Comp. Stat. 14/15(e).

78. Take-Two "profit[ed] from" Plaintiffs' and the Class members' "biometric identifier or biometric information," in violation of 740 Ill. Comp. Stat. 14/15(c).

79. By collecting, storing, using, disclosing and disseminating Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, Take-Two misappropriated Plaintiffs' and the Class members' biometrics; violated Plaintiffs' and the Class members' protected rights to privacy and personal security in their biometrics; violated Plaintiffs' and the Class members' right to information regarding Take-Two's biometrics collection and storage practices; caused Plaintiff Ricardo Vigil and numerous other Class members to incur monetary damages resulting from purchases that, had Take-Two complied with BIPA's disclosures requirements, would not have occurred; and caused Plaintiffs and the Class members to suffer a real risk of severe harm.

80. On behalf of themselves and the proposed Class members, Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Take-Two to comply with BIPA's requirements for the collection, storage, use, disclosure and dissemination of biometric identifiers and biometric information as described herein; (2) statutory damages of $5,000.00 for the intentional and reckless violation of BIPA pursuant to 740 Ill. Comp. Stat. 14/20(2), or alternatively, statutory damages of $1,000.00 pursuant to 740 Ill. Comp. Stat. 14/20(1) if the Court finds that Take-Two's violations were negligent; and

(3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 Ill. Comp. Stat. 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Vanessa Vigil and Ricardo Vigil, on behalf of themselves and the proposed Class, respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel;

B. Declaring that Take-Two's actions, as set out above, violate BIPA, 740 Ill. Comp. Stat. l4/1.

C. Awarding statutory damages of $5,000.00 for each and every intentional and reckless violation of BIPA pursuant to 740 Ill. Comp. Stat. 14/20(2), or alternatively, statutory damages of $1,000.00 pursuant to 740 Ill. Comp. Stat. 14/20(1) if the Court finds that Take-Two's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, inter alia, an order requiring Take-Two to collect, store, and use biometric identifiers or biometric information only in compliance with BIPA;

E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: July 15, 2016

Respectfully submitted,

By: /s/ John C. Carey

CAREY RODRIGUEZ MILIAN GONYA, LLP

John C. Carey (NY Bar No. JC-4639)
jcarey@careyrodriguez.com
David P. Milian
dmilian@careyrodriguez.com
Frank S. Hedin
fhedin@careyrodriguez.com
Ernesto M. Rubi*
erubi@careyrodriguez.com
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Telephone: (305) 372-7474
Facsimile: (305) 372-7475

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on July 15, 2016, I electronically filed the foregoing document with the Clerk of Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/John C. Carey